15

CLAIMS:

1.   A system comprising an information carrier (11) for comprising user-
information (20) and an apparatus (10) for accessing the information carrier, the information
carrier comprising an optical identifier (12) representing a physical one-way function and
authentication information (17), the apparatus comprising:

5   -   a light source (13) for challenging the optical identifier, when the information
carrier is present in the apparatus, by generating a light beam (14) incident on the optical
identifier as a challenge,

-           a detector (15) for detecting as response a speckle pattern (16) produced by the
optical identifier upon being challenged with the light beam,

10   -   a reading unit (18) for reading the authentication information, and

-           a verification unit (19) for comparing the response with the authentication
information, the authentication information being related to the response.

2.   A system as claimed in claim 1 wherein the user-information (20) present in

15   the information carrier (11) is encrypted, and in the apparatus (10):

-           the reading unit (18) is further capable of reading the user-information,

-           a decryption key extraction unit (25) is present, for extracting a decryption key
from the response, and

-           a decryption unit (26) is present, for decrypting the user-information encrypted

20   with the decryption key.

3.   A system as claimed in claim 1, wherein:

-           the apparatus (10) is able to provide a set of challenges, the challenges giving
rise to corresponding responses, and to detect the corresponding responses,

25   -   the authentication information (17) is further related to the corresponding
responses, and

-           the verification unit (19) is able to compare the corresponding responses with
the authentication information.

16

4.   A system as claimed in claim 3, wherein the apparatus (10) is able to select a subset of challenges from the set of challenges, to challenge the optical identifier (12) with challenges belonging to the subset of challenges, and to detect a subset of corresponding responses.

5.   A system as claimed in claim 3, wherein the authentication information (17) is further related to the set of challenges.

6.   A system as claimed in claim 5, wherein the authentication information (17) is in the form of a table (30) having a record (31) for each challenge belonging to the set of different challenges, the record having in a first field (32) the result of a first one-way function applied to the each challenge, and in a second field (33) the result of a second one-way function applied to the corresponding response.

7.   A system as claimed in claim 6, wherein the verification unit (19) is able to execute, for the each challenge, the following steps:

-          applying the first one-way function to the each challenge to obtain a first result,

-          applying the second one-way function to the corresponding response to obtain a second result,

-          identifying a record (31) in the table (30) having in the first field (32) a value equal to the fist result, and

-          reading from the record (31) identified the value present in the second field (33), and comparing it with the second result.

8.   A system as claimed in claim 1, wherein the apparatus (10) comprises means for monitoring a time (27) elapsing between challenging the optical identifier (12) and detecting the speckle pattern (16).

9.   An information carrier (11) for comprising user-information (20), the information carrier comprising an optical identifier (12) representing a physical one-way function which is able to produce a speckle pattern (16) as a response upon being challenged with a light beam (14) as a challenge, and further comprising authentication information (17) related to the response.

17

10.   An information carrier (11) as claimed in claim 9, wherein the user-information (20) is encrypted and is decryptable with a decryption key extractable from the response.

11.   An apparatus (10) for accessing an information carrier (11) for comprising user-information (20), which information carrier comprises an optical identifier (12) representing a physical one-way function and authentication information (17), comprising:

-        a light source (13) for challenging the optical identifier with a light beam (14) as a challenge,

-        a detector (15) for detecting a speckle pattern (16) produced by the optical identifier as a response upon being challenged with the light beam,

-        a reading unit (18) for reading the authentication information, and

-        a verification unit (19) for comparing the response with the authentication information, the authentication information being related to the response.

12.   A method for accessing an information carrier (11) for comprising user-information, which information carrier comprises an optical identifier (12) representing a physical one-way function and authentication information (17), comprising:

-        a challenging step (42), for challenging the optical identifier with a light beam (14) as a challenge,

-        a detecting step (43), for detecting a speckle pattern (16) produced by the optical identifier as a response upon being challenged with the light beam,

-        a reading step (41), for reading the authentication information, and

-        a verification step (44), for comparing the response and the authentication information, the authentication information being related to the response.

13.   A computer program for carrying out the method claimed in claim 12.